PCT/GB 00/03409

The Patent Office

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS

10 70326

INVESTOR IN PEOPLE

REC'D 27 SEP 2000

WIPO PCT

GB00/03409

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

4

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-[illegible]stration under the Companies Act does not constitute a new legal entity but merely s[illegible] the company to certain additional company law rules.

Signed [signature]

Dated 07 September 2000

Patents Form 1/77

Patents Act 1977

RECEIVED 06 SEP 1999

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

1/77

The Patent Office
Cardiff Road
Newport
Gwent NP9 1RH

07SEP99 E474766-1 D00060
P01/7700 0.00 - 9921029.6

1. Your reference	TRC/BP5795356		
2. Patent application number *(The Patent Office will fill in this part)*	**9921029.6**		
3. Full name, address and postcode of the or of each applicant *(underline all surnames)*	UNIVERSITY OF BRISTOL 4TH FLOOR SENATE HOUSE TYNDALL AVENUE BRISTOL BS8 1TH		
Patents ADP number *(if you know it)*	00798181001.		
If the applicant is a corporate body, give the country/state of its incorporation	GB		
4. Title of the invention	COMMUNICATION NETWORKS		
5. Name of your agent *(if you have one)*	MEWBURN ELLIS		
"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*	YORK HOUSE 23 KINGSWAY LONDON WC2B 6HP		
Patents ADP number *(if you know it)*	109006		
6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number	Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*
7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application		Date of filing *(day / month /year)*
8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:* *a) any applicant named in part 3 is not an inventor, or* *b) there is an inventor who is not named as an applicant, or* *c) any named applicant is a corporate body.* *See note (d))*	YES		

COMMUNICATION NETWORKS

The present invention relates to communication networks, and in particular, to communication networks in which terminals and/or users are mobile in the network. The present invention is applicable, for example, to the Internet where a terminal or user moves from one site to another. The present invention is also applicable to mobile telecommunication devices such as wireless telephones.

Mobility management is an essential and integral part of mobile communication networks in order to ensure terminal mobility as a minimum requirement. Two distinct sets of functions need to be provided, namely location management and handover functions. Location management functions are required to keep track of mobile terminals/users as they roam and also locate them when there is a request for a connection to them. Handover functions take care of maintaining ongoing connections as users move and change their point of attachment in the network.

It is envisaged that mobile communication systems will need to possess characteristics that are far more advanced than those presently available in current systems. In effect, global and seamless roaming of users across a completely heterogeneous environment is desirable, where different network operators and service providers co-exist. These different networks may need to operate at different

techniques and addressing schemes. In order to do global mobility management, it is necessary to analyse aspects of routing and connection set-up, addressing, signalling and database access for different networks. In cellular systems, location management relies on a structure of databases consisting of the HLR (Home Location Register) and VLR (Visitor Location Register). Queries to the databases enable exact positioning of the mobile terminal prior to set-up of a connection. This ensures that the connection is set up along an optimal route. In data networks CDPD (Cellular Digital Packet Data), GPRS (General Packet Register Service), Mobile IP (Internet Protocol), generally routing to mobile stations is done inefficiently. Packets are always routed to the home network of the mobile terminal irrespective of whether the mobile terminal is in its home network or not. The packets are forwarded to the current location of the mobile terminal from the home network. This feature is known as triangular routing. The first objective of the research is to build an efficient mobility management strategy in data networks, specifically IP, in order to overcome the sub-optimal routing problems. This can then be extended to integrate IP with other systems. For global mobility management, there is also a need to provide a means for global addressing to accommodate the different types of addresses used by different networks. The use of the IPv6 address space for that purpose is envisaged.

of two phases: mobile tracking and mobile locating. Mobile tracking essentially involves mobile terminals notifying the network of their current location and network entities updating the information accordingly. Mobile locating is the process whereby a specific query is launched in order to determine the position of the mobile prior to setting up a connection. The location management strategy, which is dictated by the approach to mobile tracking and locating, has a direct impact on the efficiency of routing in the network, the amount of signalling traffic generated and the number of accesses to databases which are used for mobility management.

As was discussed in the report by A.Sesmun, L.Q.Liu, M.Fuente, S.Vahid and A.Munro, "Examination of mobility management techniques in current systems and outline proposals for further research", Mobile VCE Networks Programme, Deliverable MVCE/BRS/WPN01/D12, May 1998, different networks have different mobility management schemes but in essence, two approaches can be identified depending on how the mobile locating phase is carried out. In cellular networks, mobility management relies on a structure of databases to keep track of mobile terminals as they roam. Upon a need to establish a connection to a mobile terminal, an explicit locating phase is required to determine the position of the terminal. In the Internet, the mobility management protocol Mobile IP integrates the mobile

(iv) the database architecture for mobility management purposes.

Different networks also have different addressing schemes. Telephone numbers follow the E.164 specification of the International Telecommunications Union. Internet addresses, usually known as IP addresses, are of two protocol versions, IPv4 and IPv6 and are used to refer to host interfaces rather than endpoints. These versions are published on the Internet at www.ietf.org. The Network Service Access Point format as specified by the International Standards Organisation is used for addressing in ATM networks. A global location management scheme would therefore require a uniform addressing scheme in order to recognise terminals in different networks.

In the Mobile IP protocol known as proposed by the Internet Engineering Task Force, a mobile is always identified by its home address, irrespective of its point of attachment in the network. When the mobile moves to a different subnet, or a foreign subnet, it acquires a temporary address referred to as a care-of-address. It then needs to register this address with its home agent by sending a binding update to the router. The home agent is a router on the mobile terminal's home link. Thereafter, the home agent can intercept any packets intended for the mobile and forwards them to the mobile's current location. This is

permanent address and the care-of-address of the mobile. The home agent keeps a record of the binding. A resource record in the name server only stores the name of a terminal and its permanent address (and also other fields not relevant here).

When a correspondent node wants to communicate to a mobile node (or a fixed node), the correspondent node need not know if the recipient is mobile or not. The correspondent node supplies an application with the name of the host. This results in a query launched to the name server, and resolution of the name to an address yields the permanent address as a response. The correspondent node uses the permanent address to send packets to the mobile node. The home agent intercepts these packets and tunnels them to the mobile node. This routing via the home agent is sub-optimal. If the mobile node is using a co-located care-of-address, the end of the tunnel is the mobile node. If the mobile is using a foreign agent care-of-address, the end of the tunnel is the foreign agent, in which case the foreign agent extracts the packet and sends it to the mobile. Subsequent routing optimisation takes place in mobile IPv6.

The present invention departs from this by considering the fact that networks each have a name server associated therewith. In the existing systems, the name server is not used in location management. The present invention, in its first aspect, proposes that the name server is used in a way

is currently located.

Thus, according to this first aspect, the present invention may provide a method of operating a network, the network comprising a domain having a name server associated therewith, said domain having a plurality of subnets, wherein:

a mobile terminal is associated with said domain and with a first subnet within said domain, said name server stores a name for said mobile terminal, a permanent address for said mobile terminal, and a second address which includes an identification of said first subnet, whereby input to the network of said name for said mobile terminal causes said name server to output said second address;

when said mobile terminal moves to a second subnet within said domain, said name server changes said second address to a third address which third address contains an identification of said second subnet, whereby input to the network of said name for said mobile terminal causes said name server to output said third address.

This first aspect will be referred to subsequently as one-level updating; the care-of-address is updated each time the mobile terminal moves from one subnet to from one subnet to another, whether that subnet is in its home domain or in a foreign domain. With this system, when a correspondent wishes to communicate with the mobile terminal, a query is launched to the name server and the address returned is the

locally.

A further development of this first aspect of the present invention considers the case where the mobile terminal moves to a foreign domain. If there is one-level updating, as previously discussed the care of address of the home name server reflects the foreign subnet in which the mobile terminal is now located. However, that foreign network itself has a name server which, as previously mentioned, may store a local address for the mobile terminal. Therefore, in this development of the first aspect of the present invention, it is proposed that, when a mobile terminal moves to a foreign network, the care-of-address thus generated is stored at the foreign name server, and a binding update, which is an association between the permanent address of the mobile and the address of the foreign name server is sent to the home agent. The address of the foreign name server then becomes the care-of-address in the home name server. Thus, in this development, when the mobile terminal moves to a foreign name server, it has a care-of-address stored in the foreign name server of that domain, and the home name server stores its permanent address and the address of the foreign name server of the domain in which it is moving.

Effectively, this system may be considered to be one in which the name server of the domain in which the mobile terminal is located stores a care-of-address for the mobile terminal, and the home name server stores either the address

Thus, when it is desired to communicate with a mobile terminal, a query is sent to the home name server. Assume now that the mobile terminal is, in fact, under the authority of a foreign name server. The home name server then identifies the foreign name server, so that signals may then be sent to that foreign name server to identify the current care-of-address. The home name server does not need to know the current care-of-address. Once the correspondent obtains the care-of-address of the mobile, communication can be established directly and the home network can be bypassed. It should be noted that the term "foreign" merely means a part of the Internet served by a name server which is not the original name server of a particular mobile terminal.

Preferably, the home name server continues to store a permanent address for the mobile terminal, so that the address of the foreign name server may be stored in the same field which stores a care-of-address when the mobile terminal moves within the domain served by the home name server. In effect, the address of the foreign name server replaces the care-of-address when the mobile moves from the domain served by the home name server to a domain served by the foreign name server. This is the two-level updating previously mentioned.

It should be noted that the Domain Name System is the distributed name service used in the Internet, which

However, the idea of using the address of the local name server as the care-of-address within the home name server may be considered a second independent aspect of the present invention.

Thus, in the second aspect, the present invention may provide a method of operating a network, the network comprising a plurality of interlinked domains, each domain having a name server associated therewith, each domain having at least one subnet, wherein:

a mobile terminal is first associated with one of said domains and a first subnet within said one of said domains, the name server of said one of said domains storing a name for said mobile terminal and an address of said mobile terminal, which address includes an identification of said first subnet, whereby the input of said name for said mobile terminal causes said name server said one of said domains to output said address;

when said mobile terminal moves to a second subnet associated with a second one of said domains, the name server of said second one of said domains stores said name for said mobile terminal and another address for said mobile terminal, which another address includes an identification of said second subnet, and said name server of said one of said domains stores said name of said mobile terminal and an address of said name server of said second one of said domains, whereby the input to the network of said name for

In the third aspect of the present invention, cellular telephone domains have name servers associated therewith, in the same way as Internet networks. As for the Internet, the name servers define a domain over which they have authority and provide coverage. The domain servers are accessible by all networks, and are identified by a suitable address. When the domain is a cellular telephone domain, the E.164 number forms the name of the mobile telecommunications device within that domain. Where the domain is an Internet domain, the name is the normal Internet one. Each name server then associates with the name a permanent address and a temporary address. The temporary address may be the current care-of-address of the terminal, or may be the address of another name server, which holds the current care-of-address. Thus, by providing name servers associated with cellular telephone domains, having an addressing system corresponding to that of the first aspect, but provided across all types of domains, a global communication system across different networks can be achieved.

Embodiments of the present invention will now be described in detail, by way of example, with reference to the accompanying drawings, in which:

Fig. 1 is a tree diagram showing an Internet naming hierarchy;

Fig. 2 is a schematic network diagram showing the movement of terminals in an Internet network;

Fig. 15 shows the structure of an IPv6 address;

Fig. 16 shows the structure of an integrated E. 164/IP address;

Fig. 17 shows the structure of a network involving Internet and other mobile communications; and

THE FIRST EMBODIMENT

The first embodiment of the present invention will now be described, being an Internet communication system.

In the Internet, users typically supply applications with a destination's name rather than an address. Applications then need to resolve the name to an address by sending a query to a name server, which responds with the translation to an address. Upon receipt of the address, transmission of traffic to that address can be initiated. Generally, the name server stores the mapping from name to permanent address for a host. The proposed approach is to modify the name server such that it not only stores the permanent address of a host but also its care-of-address, indicating current location of a mobile terminal (hereinafter "mobile"). A query to the name server would then provide an application with an address identifying its current point of attachment and packets can be sent directly to the host, bypassing the home subnet. A more optimal route can be used.

The Domain Name System, more specifically the name servers, provide a suitable structure of databases, where a

acquires a care-of-address in a similar way as defined for Mobile IP. The foreign agent registers the arrival of this mobile in the local or foreign name server, which adds an entry relating to that host. This update ensures that if any host within that subnet needs to communicate to the mobile, a query to the name server can be resolved locally, thus minimising the traffic generated. The local name server is acting as a Visitor Location Register.

Location update: After acquiring a care-of-address, the mobile host needs to inform the home agent of its new point of attachment. It sends a binding update to the home agent, giving its current care-of-address. Besides keeping a record of the binding, the home agent is now also responsible for updating the local name server within that subnet. The care-of-address field of the record corresponding to the mobile needs to be updated accordingly. This takes care of the mobile tracking phase when 1-level updating is used. That name server acts as a Home Location Register for the mobile. When 2-level updating is used, the home agent receives a binding update only when the mobile terminal changes domains and the home name server stores the address of the foreign name server instead of the care-of-address of the mobile.

Mobile locating: When a user needs to launch an application that connects to another terminal, a query is initiated as normally is to determine the address of the destination. The resolver tries to find an answer locally,

router, that is the foreign agent, as well as the home agent of its new location. The foreign agent can update the local name server accordingly. Furthermore, it can intercept any packets destined for that mobile and can forward them to its current location. When the mobile detects that it is receiving packets that are being forwarded, it can also send a binding update to the correspondent node, which can use its care-of-address for any subsequent transmission, thereby ensuring optimal routing.

Binding updates: Every binding update is associated with a time to live which then determines for how long the entry in a name server is valid. After the expiration of that time, any resource records that are no longer valid are deleted provided the name server is not an authoritative server for these hosts. The authoritative server remains the name server in the home subnet of the host and after expiration of the time to live, the care-of-address is set back to the permanent address of the host.

Consider now the simplified Internet shown in Fig. 2. In Fig. 2, a correspondent node 10 seeks to communicate with a mobile node 11. The home agent of the mobile node is shown at 12, and the home name server of the mobile node 11 at 13. In the situation envisaged by Fig. 2, the mobile node has moved from its home network to a foreign network, which foreign network has a foreign name server 14 controlled by a foreign agent 15. For any mobile terminal, there needs to

needs to register this new care-of-address with its home agent. The mobile host sends (step 101) a binding update (BU) where the following fields are set as shown to the home agent.

Option: binding update
Source: care-of-address of mobile node
Destination: address of home agent
Care-of-address: care-of-address of mobile node
H flag bit: set (host address)
Home address option: permanent address of mobile node
Lifetime: time duration for which this update is valid
Additional option required: name of mobile node

The foreign agent 15 intercepts any binding updates (step 102) and processes them in the following way. First the foreign agent 15 sends a query (step 103) to the local name server 14 (which in this case is the foreign name server) to find out if a record of the mobile node 11 is held in the database. The recursion desired (RD) bit should not be set in the query to ensure that the query is resolved locally and no recursion is carried out. If there is no entry in the database of the local name server 14, the result sent back to the foreign agent 15 is a name error. The foreign agent then adds an entry in the name server (step 104), giving the following information:

Name of mobile node

Name of the mobile node

Permanent address

Address of local name server

Type of temporary address (name server address)

Lifetime of entry.

This results in the temporary address, type of address and time to live (lifetime) fields being set to the values provided.

The steps described above take care of the location updating procedure when the foreign agent is 2-level location updating enbabled. In case only a single type of location updating is used, the foreign agent 15 relays any binding updates it receives from a mobile node to the home agent without doing any processing. The home agent 12 updates the home name server 13 when it received the update such that the temporary address associated with the mobile host is its actual care-of-address.

Thus, when a correspondent host wants to communicate to a host (mobile or fixed), the application will typically be supplied with the name of the host. If the application is supplied with the address of the host and this host is mobile and has moved away from its home network, the correspondent host will eventually be informed of the address of the mobile node via Mobile IPv6 operation. If a name is supplied, a query is launched to the name server to

and end users. The end users can be fixed or mobile. Each router identifies a subnet in which the end users reside. A two-level addressing is being used in the current implementation so that the address of an end user is composed of a *subnet id* and a *node id*. The *subnet id* represents the subnet to which the end user belongs, in other words the router to which it is connected. The *node id* distinguishes between different end users in the same subnet. An end user, fixed or mobile, is assigned a permanent address which does not change during the course of the simulation. Mobile end users are allowed to move according to a predefined trajectory, specified in terms of speed, direction and duration of motion. End users can also be involved in packet transmission.

The name server may be implemented as a database in Oracle. The name server can be centralised or can be distributed according to a two-level hierarchy. In the latter case, at the lowest level, a name server can be responsible for a number of subnets, which constitute a domain. At the higher level, the root name server maintains information about the lower level name servers. As opposed to a traditional name server, which mainly keeps a record of the name and permanent address of a host, the one used in the simulation holds details of the name, permanent address and care-of-address of a host. In the case of a fixed host or a mobile host which is in its home subnet, the care-of-

message. Therefore, if a signalling message generated by an end user takes 4 hops to reach for example the home agent, 4 messages will be recorded. This definition is used in order to take into consideration not only the mobility of users but also the reachability of the home agent or the correspondent host from the location of the mobile user. It also takes account of the distance of the name server from the home and foreign agents in terms of connectivity.

The results to be discussed have been obtained for the network topology shown in Figure 4. Only the routers are shown but each router has a number of end users within its subnet. Communication to an end user is achieved via the router to which it is connected. At the start of a simulation, all mobile end users are in their home subnet. If a mobile user subsequently moves during the course of the simulation, it registers with different routers as it roams in different subnets. The point at which a mobile enters a different subnet is identified when the distance between the mobile and the new router is shorter than its distance from the router it is presently connected to. A central name server is used, which is located at router 0. This name server is the authoritative server for the entire domain and maintains records of name, permanent address and care-of-address for all users in the network.

The scenario used in the simulation is as such. A mobile terminal denoted by *user A*, attached initially to router 2

IPv6 and the approach of the embodiment of the present invention. In effect, with signalling load as defined and upon application of the particular scenario described above, Mobile IPv6 shows a 65% increase in signalling load as compared with Mobile IPv4 whereas the DNS approach of the embodiment of the invention shows an increase of 132%. The increase in signalling load in Mobile IPv6 is due to the fact that binding updates are now sent not only to the home agent but also to the correspondent host. The approach of the embodiment of the present invention exhibits a 41% increase in signalling load as compared to Mobile IPv6. This arises solely because of the messages required to send updates to the name server. Given its definition, the signalling load is dependent on the location of the mobile with respect to its home network and the correspondent host. The further away the mobile is from both its home agent and the correspondent host, the more signalling traffic is generated. Signalling load is also dependent on the location of the name server with respect to the home agent and foreign agents. A centralised name server implies that more signalling traffic is generated if the home agent is far away in terms of connectivity from the server. A distributed architecture for the name server would alleviate the load due to access to the name server.

A second scenario has been investigated using one-level updating as previously described, whereby a user denoted by

is still at home. Subsequently, the number of hops is expected to be equal to 4, 3, 2 and finally 3 as the mobile changes its point of attachment in the network.

However, the optimality of the route taken depends on the mobility management protocol. In Mobile IPv4, the correspondent host is never informed of the location of the destination and always sends packets via the home agent. As a result, packets may take a minimum of 5 hops when the mobile is at home to a maximum of 8 hops when the mobile is in effect roaming in the same subnet as the source. In Mobile IPv6, the situation is improved given that as the mobile changes location, it sends a binding update to the home agent, its previous default router as well as the correspondent host. Still, initial transmission of packets assumes that the mobile is at home, which leads to packets being forwarded to their destination from router 2. The new approach that is being proposed eliminates the initial triangle routing so that provided the name server has been updated in time, packets are expected to reach their destination after a maximum of 5 hops.

In all three simulations, when packet transmission starts, the mobile has reached router 0. 200 packets were transmitted. The average number of hops required for a packet to arrive at its destination is summarised in Figure 8 in which "DNS scheme" refers to the approach of this embodiment of the present invention.

Figure 9. The home agent is assumed to be located in region *A*. The correspondent node resides in region *C* and does not move during the course of transmission of traffic. The number beside the link between two entities indicates the number of hops separating them.

Three cases are considered, in which the mobile terminal is located in each of the three regions. For example, in the first case, the mobile terminal is located in region *A*, 2 hops away from the home agent and 12 hops away from the correspondent node. Results are obtained when the mobility management protocol is based on Mobile IPv6 and on the approach of the present invention. This procedure is repeated for the cases where the mobile resides in regions *B* and *C*. The degree to which the approach of the present invention performs better is measured in terms of the number of packets that take a sub-optimal route to the mobile terminal when Mobile IPv6 is used. These packets correspond to the number of packets that are sent via the home agent before the correspondent node receives a binding update about the location of the mobile. The results are summarised in Figure 10.

As can be seen, the number of packets that are transmitted to the mobile terminal via the home agent and therefore take a sub-optimal route depends on the location of the mobile with respect to its home network and the correspondent node.

an impact on the signalling load associated with the proposed protocol.

Thus, the approach of this embodiment of the present invention outperforms Mobile IPv4, where routing is sub-optimal and there is no attempt at optimising routing at all. The new protocol performs better than Mobile IPv6 at the start of communication between two users because it eliminates the triangular routing. Mobile IPv6 still requires packets to be initially sent via the home network until the destination informs the correspondent host of its current location. The degree to which the proposed approach is better than Mobile IPv6 depends on the relative distance between the correspondent host, the mobile host and the home agent in terms of connectivity. The distance between the mobile host and its home network determines how quickly the mobile receives packets from its home agent. The distance between the mobile host and the correspondent host then determines how quickly it can inform the correspondent host of its new location. The combination of the number of packets that follow a sub-optimal route and the time taken for the mobile host to notify the correspondent host of its location determine the degree to which the new approach is better. This is because the proposed approach avoids any forwarding of packets and does not require the mobile host to inform the correspondent host of its initial location; a query to the name server has already made the correspondent

the distribution when both global and local updating are allowed. The number of signalling messages initiated in the network is monitored at regular time intervals, shown as number of readings on the x-axis. From the graph, it is clear that the introduction of 2 types of location updates reduces the overall signalling load associated with location updating considerably. This is due to the fact that firstly global updating only takes place when the mobile crosses domains and secondly local updating generates less signalling traffic, the databases being closer to the location of the mobile. Therefore, the scheme is especially valuable when the mobile user is roaming far away from its home network and under conditions of low mobility of users across visited domains.

However, the gain achieved in terms of the reduction in location update traffic is offset by an increase in the traffic generated to locate the mobile when there is a need to send traffic to that user. In effect, for the same simulation, a 2.3% penalty is incurred in the total signalling traffic in the network when one call to the mobile user is included. The degree to which the mobile locating associated traffic increases depends on whether the correspondent node and the mobile node belong to same domains or not and also on the way in which the query is resolved. In the simulation considered, the resolver was operating in the non-recursive mode.

destination code (NDC) and a subscriber number (SUBNET), as shown in Fig. 13. The length of the country code varies between 1 and 3 digits.

The country code identifies the destination country. A combination of the national destination code and the subscriber number constitutes a national significant number, which identifies the destination subscriber.

Assignment of *country codes* falls under the responsibility of ITU. Each country's naming authority is then allowed to choose *area codes* and for each area, each central office is given an *exchange number*. Finally, the last four digits of a telephone number are assigned to a particular local loop from a central office to a subscriber. Therefore, the numbering scheme for telephones in the world follows a hierarchical structure.

In GSM, a mobile subscriber is identified by its mobile station ISDN number (MS-ISDN) and its International Mobile Subscriber Identity (IMSI). The MS-ISDN has the same structure as an E.164 number, including a country code, a national destination code and a subscriber number. The national destination code is allocated to GSM PLMN. A combination of the country code and the national destination code provides routing information to the HLR of the mobile. The IMSI is assigned to each authorised GSM user. It consists of a mobile country code (MCC), a mobile network code (MNC) and a PLMN unique mobile subscriber identification number (MSIN)

reservation of a portion of the address space for that type of addresses. For example, the prefix 001 denotes that the remaining portion is an aggregatable global unicast address where as prefix 1111 1111 shows that the address held is a multicast address. This is shown in Fig. 15.

The aggregatable global unicast address is designed to support both provider-based aggregation as well as a new type of exchange-based aggregation. This combination can allow efficient routing for sites that connect directly to providers and for sites that connect to exchanges. An aggregatable address is organised into a three-level hierarchy including the public topology, the site topology and an interface identifier. Thus, an IPv6 address of this format can have a topological or geographical significance.

In order to realise global and seamless roaming, it is required to develop a scheme whereby a terminal is recognised in all networks and can be reached irrespective of its point of attachment. In order to make sure that terminals are reachable anywhere, there is a need to manage the location of terminals at a global level. This calls for the deployment of databases that are accessible to all networks.

Thus, in this second embodiment of the invention the scheme devised to improve mobility management in IP is extended such that it can be used across different networks. Note that by using the arrangement of the first embodiment,

Having a combined address ensures that every telephone number has its equivalent IP address. In the mobile world, a mobile terminal is identified by its MS-ISDN number and its IMSI, which all have a maximum of 15 digits. Therefore, these numbers can be mapped on to IP addresses.

Consider now the network arrangement shown in Fig. 17, in which two systems 200, 300 are connected via the Internet 400. For simplicity, in Fig. 17 each network 200, 300 comprises a switching and routing unit 201, 301 connected to a name server 202, 302 and serving base stations 204, 205, 304, 305. Each switching and routing unit 201, 301 is connected by a respective gateway 206, 306 to the Internet 400. In Fig. 17, the networks 200, 300 can be an Internet-based system such as described with respect of the first embodiment, or a cellular network. In the following discussion, the network of the first embodiment will be referred to as an IP based system and the following abbreviations will be used:

GMSC	Gateway Mobile Switching Centre
HLR	Home Location Register
HNS	Home Name Server
IAM	Initial Address Message
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAI	Location Area Identity

integrated E.164/IP address in the case where E.164 numbers were already used to identify the location registers. The resource record corresponding to a cellular user in a name server has the following values for the fields given below:

Name:	E.164 number
Permanent address:	E.164/IPv6 integrated address
Temporary address:	E.164/IPv6 integrated address

The name is an E.164 number corresponding to the MS-ISDN number of the user. The permanent address is the IPv6 address representing the IMSI. The temporary address (in the home name server) is the IPv6 address representing the address of the VLR. Thus when a cellular user roams to an IP-based network, the foreign agent allocates an IPv6 address to it to be used as care-of-address. It does not configure its care-of-address by itself.

As has been mentioned above, there are four possibilities for a mobile terminal roving between one network and another. The protocols needed in the first case, where an IP terminal roams from one IP-based network to another have been described with reference to the first embodiment. The other three situations involve cellular issues.

Consider first the case where a cellular terminal roams between cellular systems. The following steps are needed for location management and location updating:

1. A mobile user moves into the coverage area of an MSC

which the present embodiment requires an additional updating operation.

Consider now the case where an IP terminal roams to a cellular system. This is generally similar to the first embodiment, except that the cellular TMSI must then act as the foreign agent for the mobile terminal. Thus, the steps needed for location management:

1. Mobile detects movement to a cellular system.

2. Mobile provides its IPv6 address for identification.

3. The local MSC acts as a foreign agent and may use this address for authentication.

4. Mobile acquires a new LAI and a TMSI. VLR generates the new TMSI.

5. The mobile host requests the local MSC to send a binding update to its home agent. (MSC functionality therefore needs to be enhanced.)

6. The MSC sends a binding update to the home agent with the following fields:

Source: IP address of MSC

Destination: IP address of home agent

Care-of-address: IP address of VLR

H flag: not set (address of another database)

Home address option: permanent IP address of mobile node

7. The home agent updates the home name server

the name server to identify the location of the user. The correspondent host (initiator of the connection) supplies a name or an E.164 number, from which the system determines the address of the home name server to by queried. An attempt is made at resolving the query locally, failing which the query is sent to the home name server. When the recipient host is roaming in a cellular network, and the call is to be terminated in a cellular system a query is launched to the Home Name Server. The Home Name Server refers the query to the VLR whose address it holds. The VLR returns the MSRN, which is an E.164 number, as an IPv6 address. The HNS send this IPv6 address (MSRN) to the GMSC, which is the entry point to the cellular network. The MSRN is sent back to the caller as an IPv6 address. The GMSC extracts the E.164 number, identifies the MSC via which communication should be done and sends an IAM message to the MSC supplying the MSRN (as done in cellular system). From the MSC onwards, normal cellular system operation takes place in order to page the mobile and obtain its location. The caller (correspondent) uses the IPv6 value of the MSRN for communication.

If the call is to be terminated in an IP-based system and if the recipient is accessing a wireless LAN or an IP-based system, the response from the home name server points to a local namer server that has authority over that domain. A query to the local name server would yield the care-of-

CLAIMS

1. A method of operating a network, the network comprising a domain having a name server associated therewith, said domain having a plurality of subnets, wherein:

a mobile terminal is associated with said domain and with a first subnet within said domain, said name server stores a name for said mobile terminal, a permanent address for said mobile terminal, and a second address which includes an identification of said first subnet, whereby input to the network of said name for said mobile terminal causes said name server to output said second address; and

when said mobile terminal moves to a second subnet within said domain, said name server changes said second address to a third address which third address contains an identification of said second subnet, whereby input to the network of said name for said mobile terminal causes said name server to output said third address.

2. A method according to claim 1, wherein the network has a second domain, said second domain having at least one subnet, wherein, when said mobile terminal moves to said at least one subnet of said second domain, said name server changes said second or third address to a fourth address, which fourth address contains an identification of said at least one subnet of said second domain, whereby input to the network of said name for said mobile terminal causes said

for said mobile terminal and another address for said mobile terminal, which another address includes an identification of said another subnet, and said name server of said one of said domains stores said name of said mobile terminal and an address of said name server of said second one of said domains, whereby the input to the network of said name for said mobile terminal causes the name server of said one of said domains to output the address of said name server of said second one of said domains, and causes said name server of said second one of said domains to output said another address.

5. A method according to claim 4, wherein when said mobile terminal moves to a third subnet associated with said one of said domains, said name server of said one of said domains changes said address of said mobile terminal whereby said changed address includes an identification of said third subnet.

6. A method according to claims 4 or claim 5, wherein when said mobile terminal moves to a fourth subnet associated with said second one of said domains, said name server of said second one of said domains further changes said another address of said mobile terminal, whereby said further changed address includes an identification of said fourth subnet.

having a name server associated therewith, each domain having at least one subnet, wherein,

the name server of a first one of said domains is arranged to store a name and an address for one of said mobile terminals, which address includes an identification of said first subnet, said mobile terminal being associated with said first one of said domains and a first subnet within said one of said domains, whereby the input to said communication means of said name for said mobile terminal is arranged to cause said name server of said first one of said domains to output said address; and

the name server of a second one of said domains is arranged to store said name for said one of said mobile terminals and another address for said mobile terminal when said mobile terminal moves to a second subnet associated with a second one of said domains, said another address including an identification of said second subnet and said name server of said first one of said domains is arranged to store said name of said name server of said second one of said documents and an address of said name server of said second one of said domains, whereby the input to the network of said name for said mobile terminal is arranged to cause the name server of one of said domains to output the address of said name server of said second one of said domains, and to cause said name server of said second one of said domains to output said another address.

Fig 1

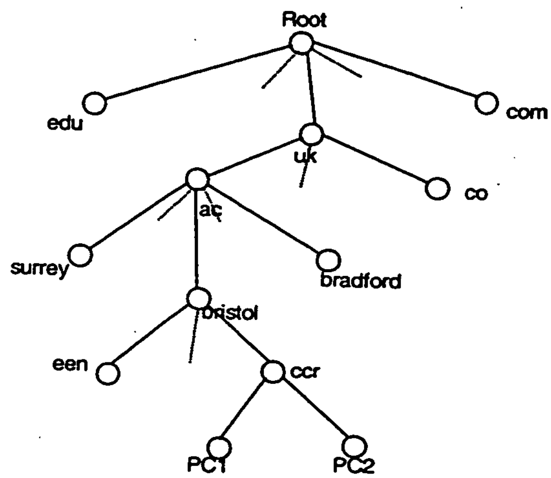

Root
edu
com
uk
co
ac
surrey
bradford
bristol
een
ccr
PC1
PC2

Fig 2

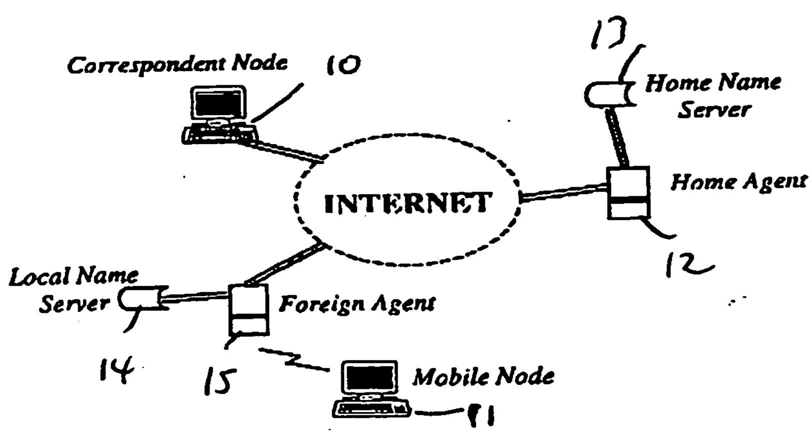
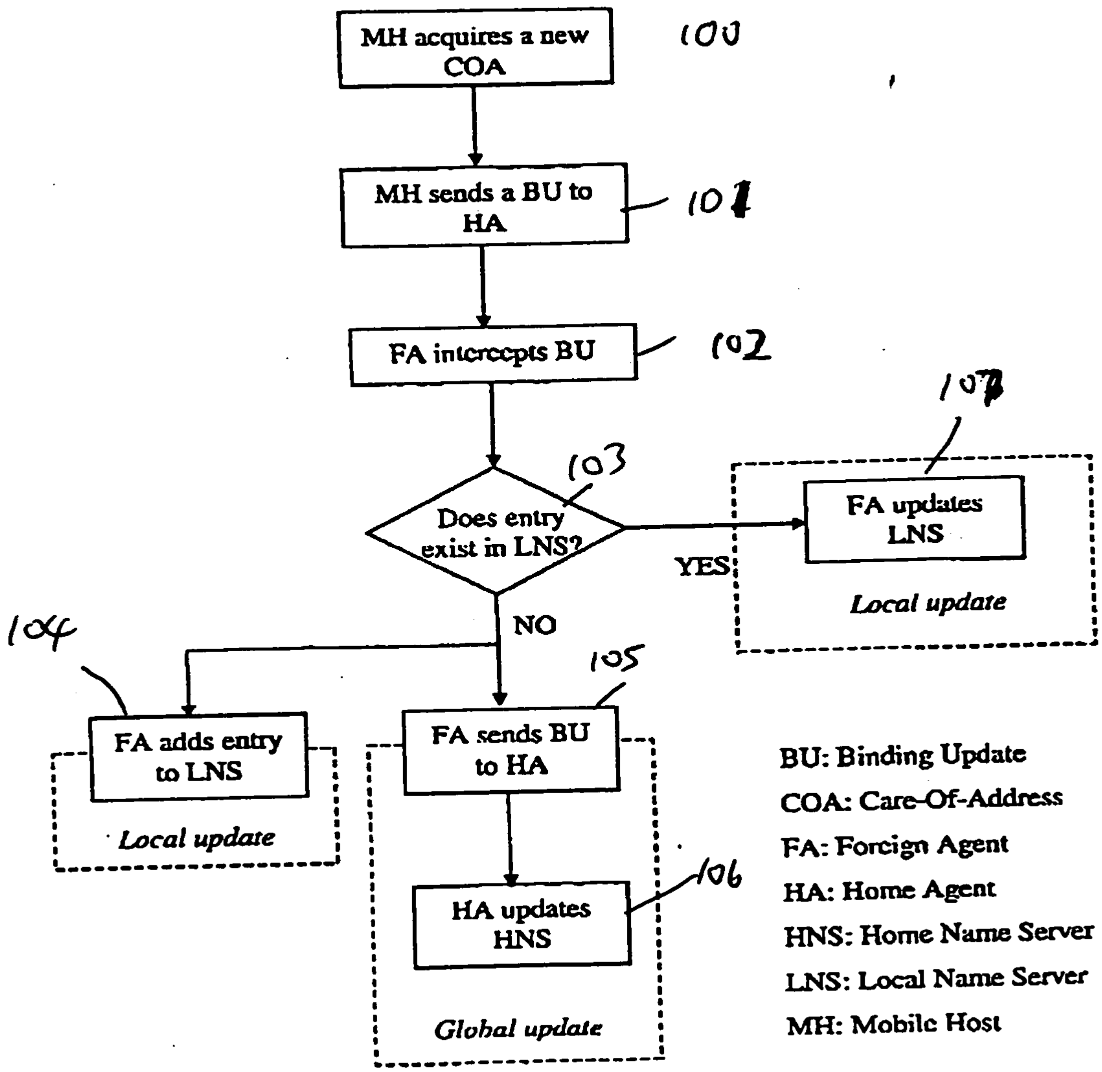
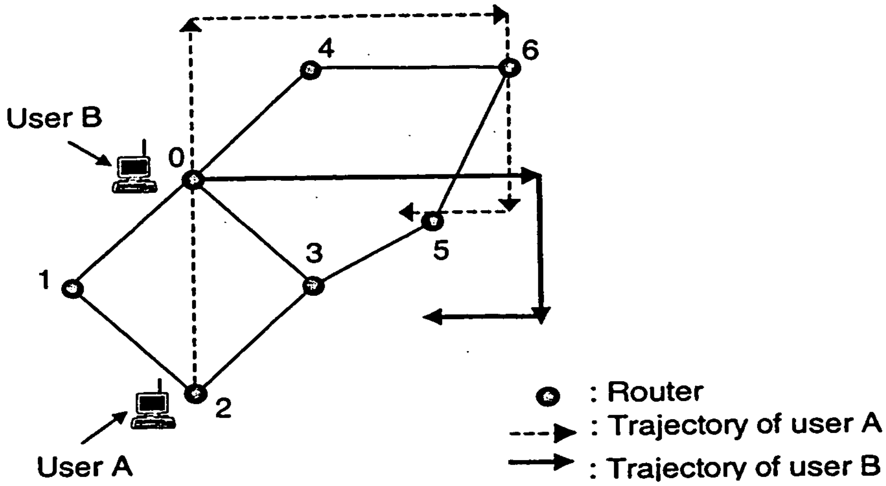

Correspondent Node
10
13
Home Name Server
INTERNET
Home Agent
12
Local Name Server
Foreign Agent
14
15
Mobile Node
11

Fig 3



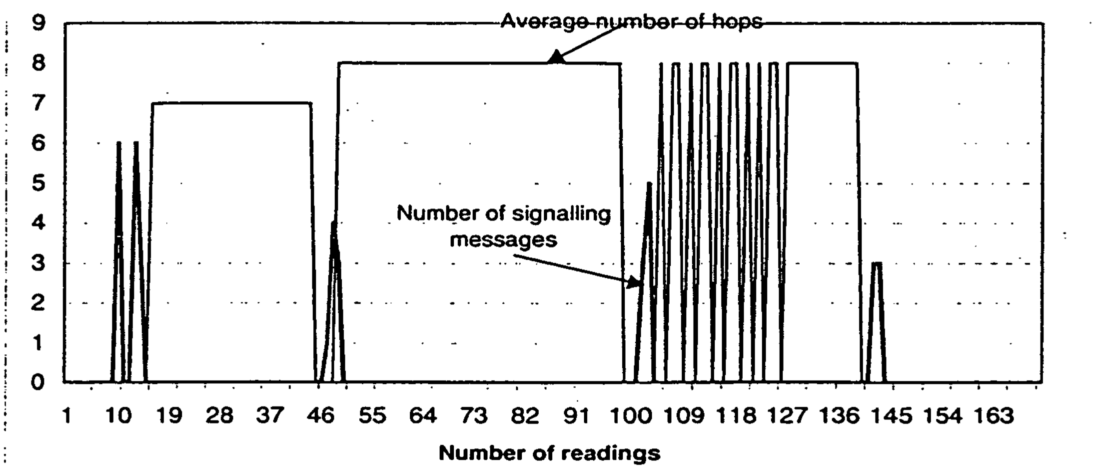
MH acquires a new COA
100
MH sends a BU to HA
101
FA intercepts BU
102
Does entry exist in LNS?
103
YES
FA updates LNS
107
Local update
NO
FA adds entry to LNS
104
Local update
FA sends BU to HA
105
HA updates HNS
106
Global update
BU: Binding Update
COA: Care-Of-Address
FA: Foreign Agent
HA: Home Agent
HNS: Home Name Server
LNS: Local Name Server
MH: Mobile Host

Fig 4



User B
0
1
2
3
4
5
6
User A
: Router
: Trajectory of user A
: Trajectory of user B

Fig 5



Average number of hops
Number of signalling messages
9
8
7
6
5
4
3
2
1
0
1 10 19 28 37 46 55 64 73 82 91 100 109 118 127 136 145 154 163
Number of readings

Fig 6

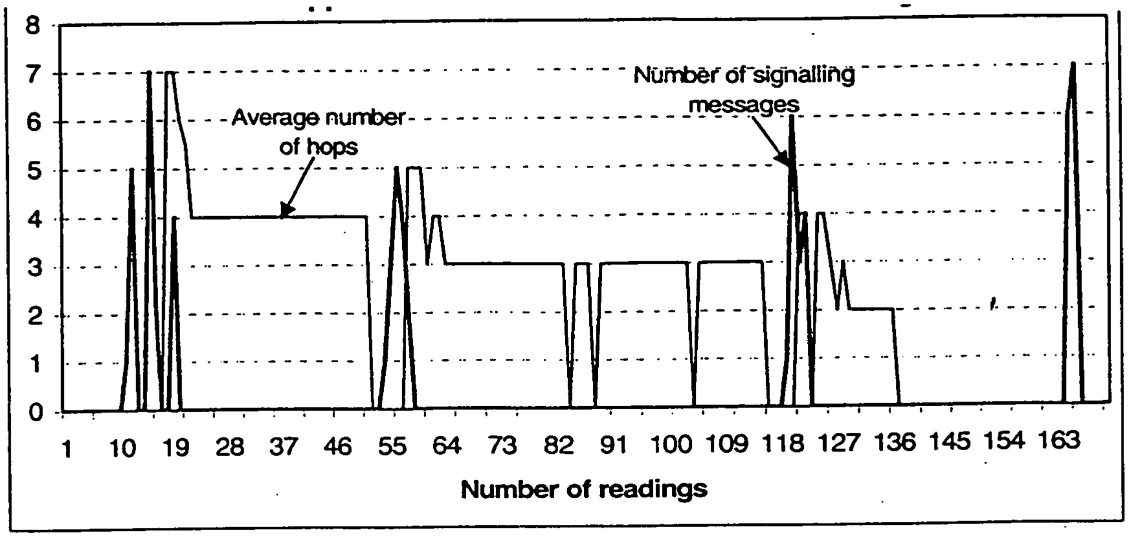

8
7
6
5
4
3
2
1
0
Number of signalling messages
Average number of hops
1 10 19 28 37 46 55 64 73 82 91 100 109 118 127 136 145 154 163
Number of readings

Fig 7

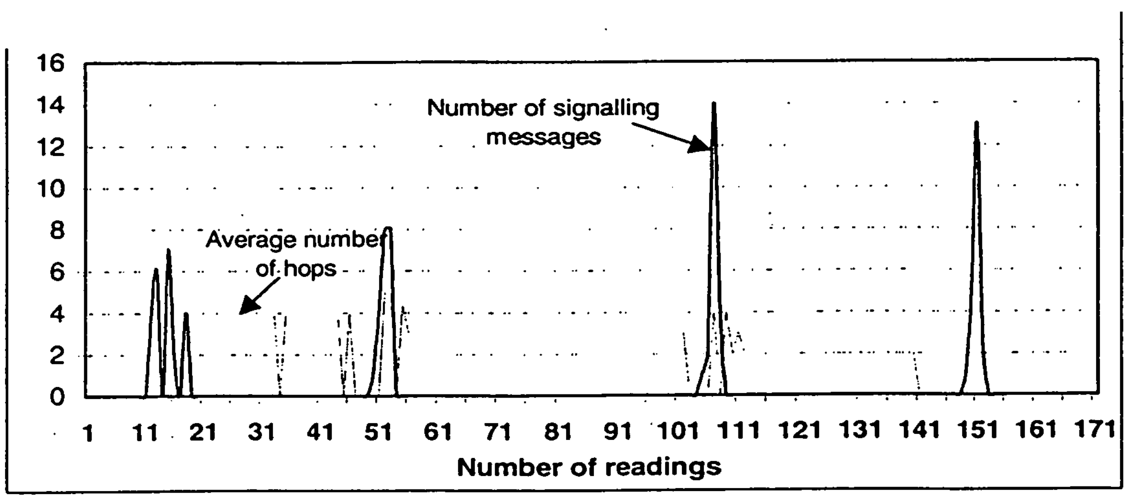
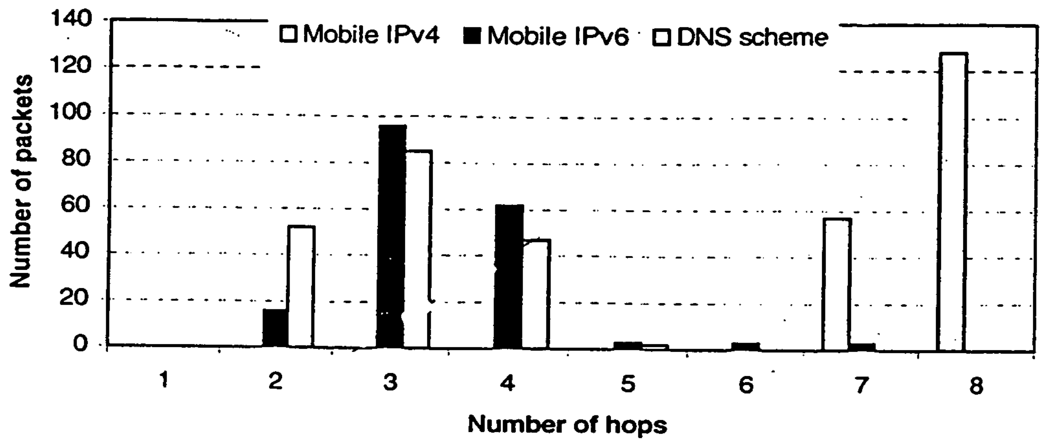
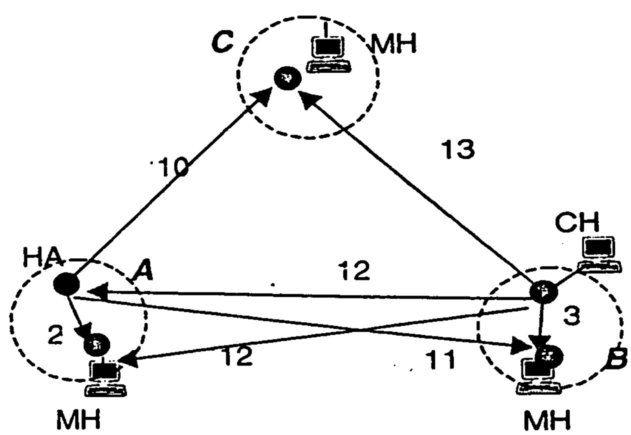

16
14
12
10
8
6
4
2
0
Number of signalling messages
Average number of hops
1 11 21 31 41 51 61 71 81 91 101 111 121 131 141 151 161 171
Number of readings

Fig 8



140
120
100
80
60
40
20
0
Number of packets
Mobile IPv4
Mobile IPv6
DNS scheme
1
2
3
4
5
6
7
8
Number of hops

Fig 9



C
MH
10
13
CH
HA
A
12
2
3
12
11
B
MH
MH

Fig 10

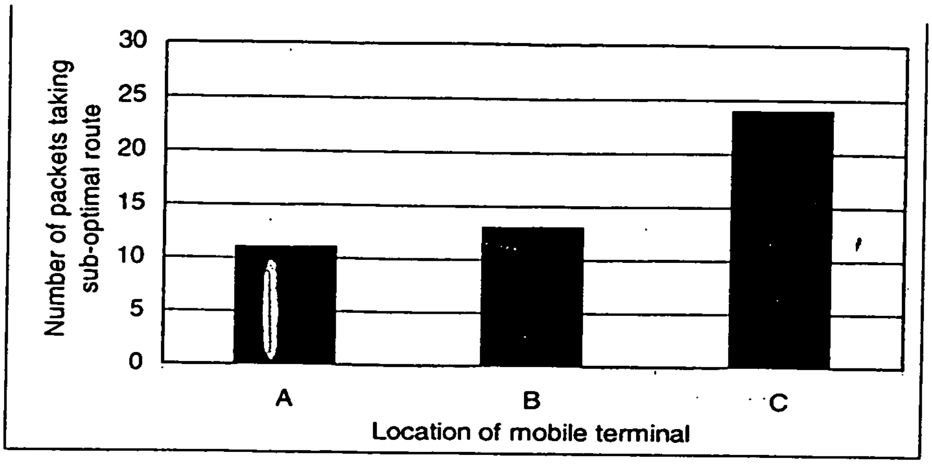


Fig 13

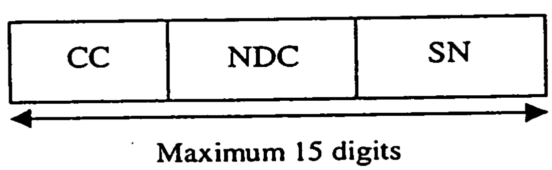


Fig 14

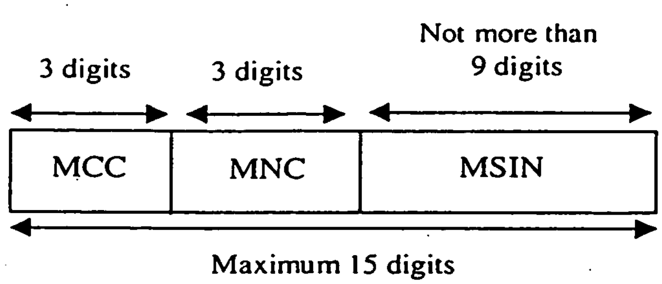
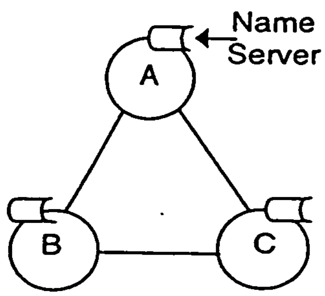
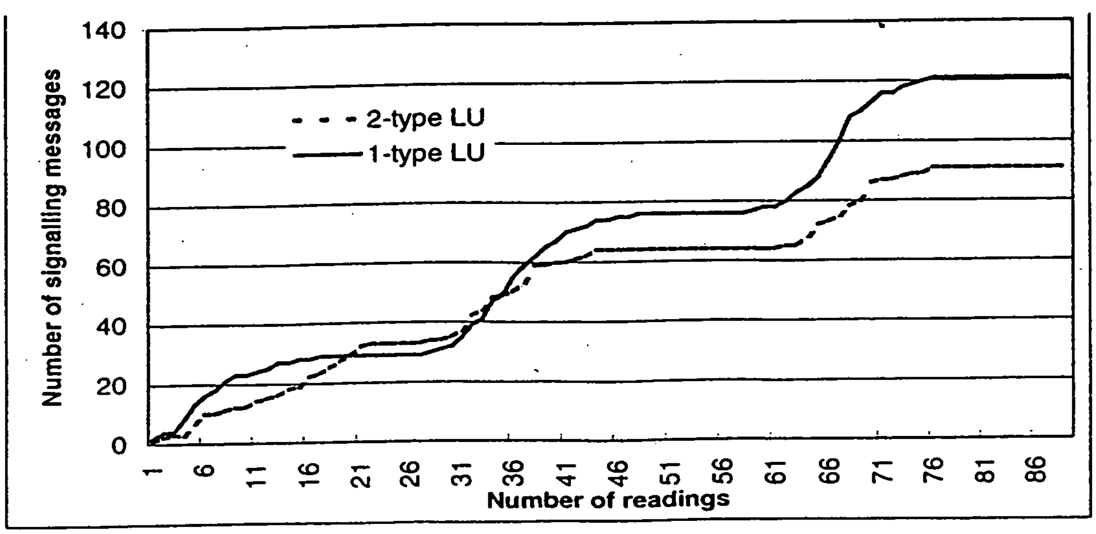


Fig 11



Name Server
A
B
C

Fig 12



140
120
100
80
60
40
20
0
Number of signalling messages
2-type LU
1-type LU
1
6
11
16
21
26
31
36
41
46
51
56
61
66
71
76
81
86
Number of readings

Fig 15

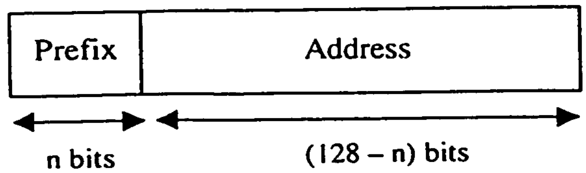


Fig 16

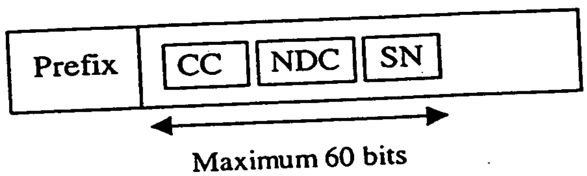


Fig 17